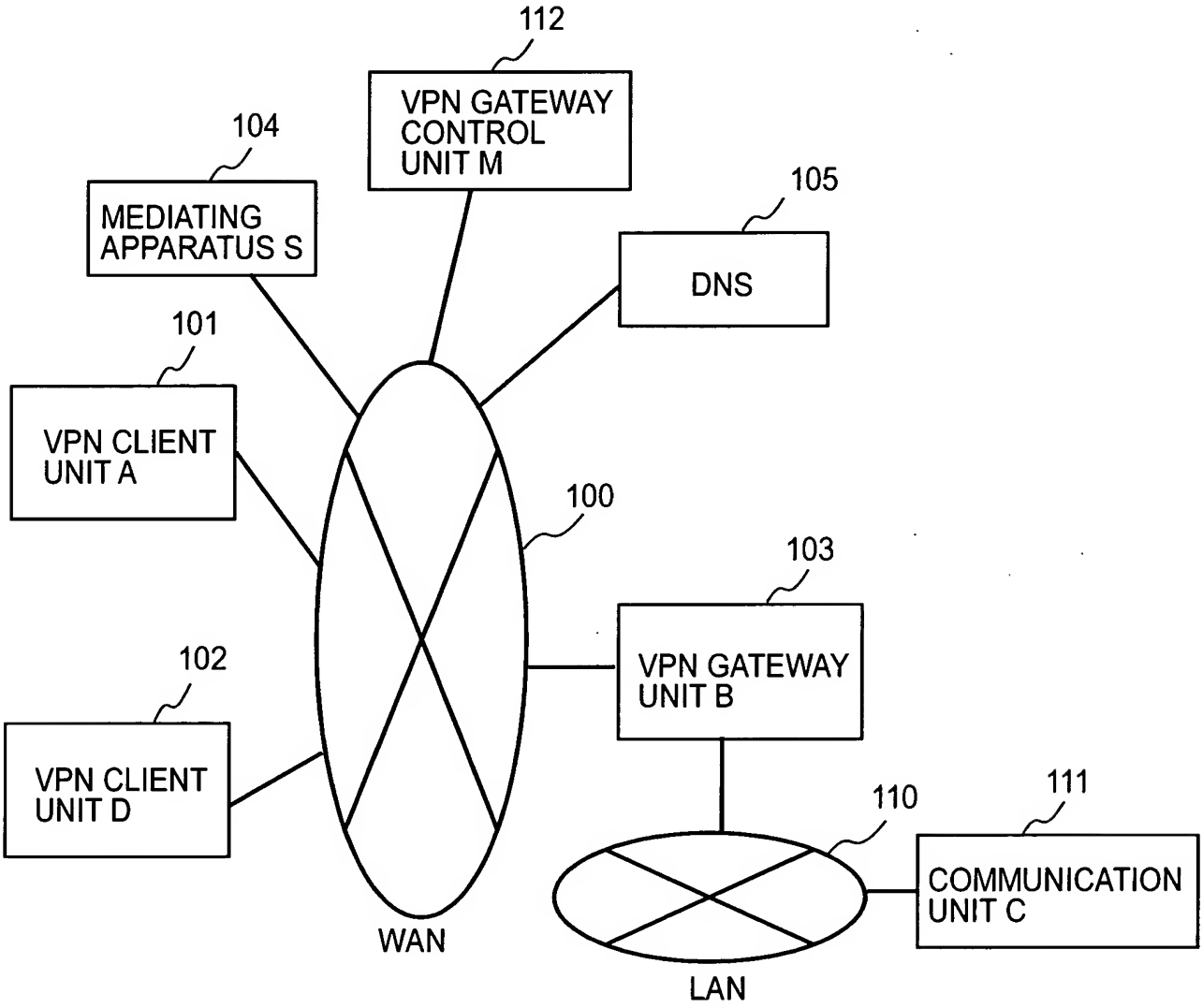

112
VPN GATEWAY CONTROL UNIT M
104
MEDIATING APPARATUS S
105
DNS
101
VPN CLIENT UNIT A
100
103
VPN GATEWAY UNIT B
102
VPN CLIENT UNIT D
110
111
COMMUNICATION UNIT C
WAN
LAN

FIG. 1

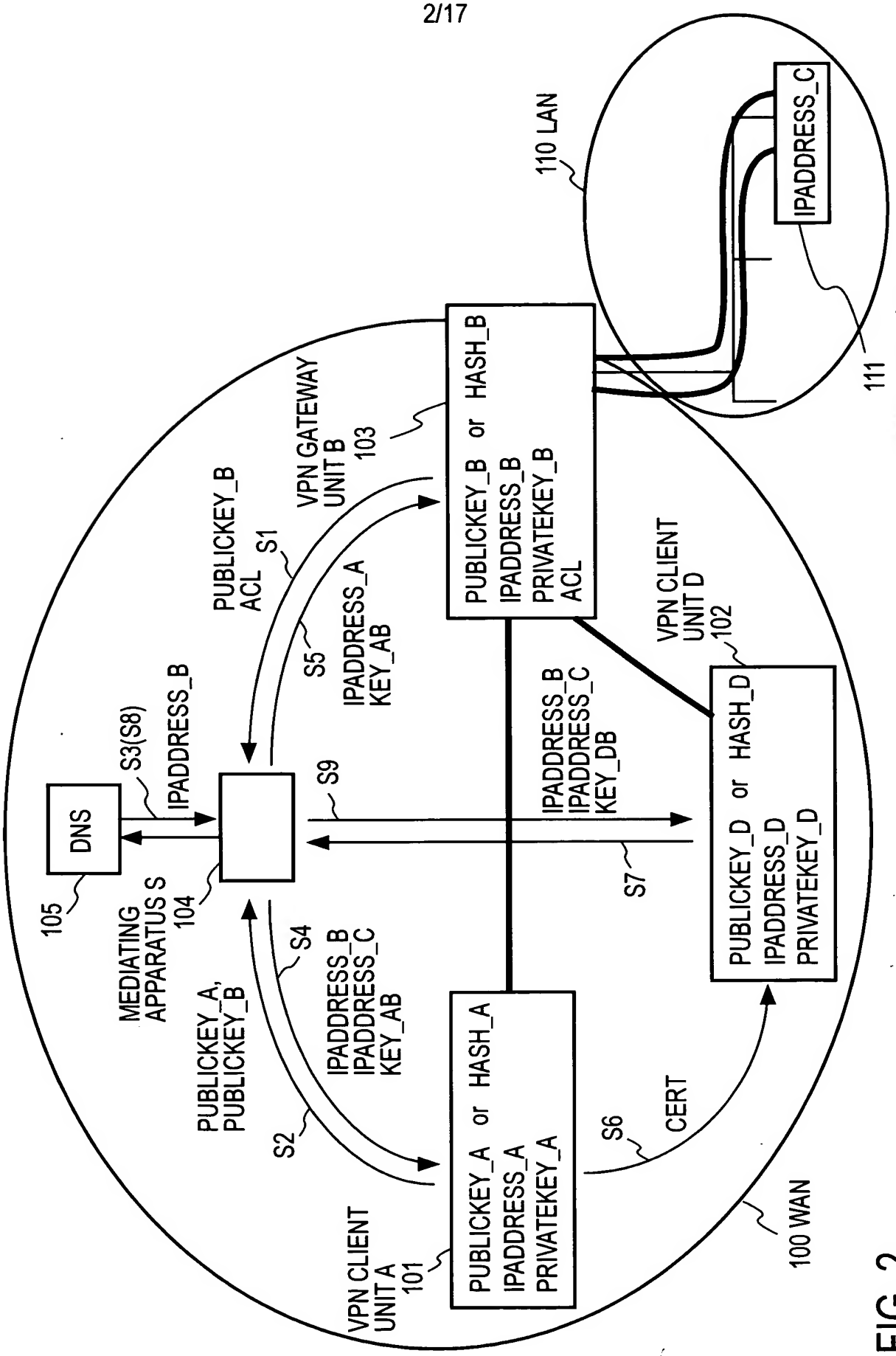

110 LAN
IPADDRESS_C
111
COMMUNICATION UNIT C
VPN GATEWAY UNIT B
103
PUBLICKEY_B or HASH_B
IPADDRESS_B
PRIVATEKEY_B
ACL
PUBLICKEY_B
ACL
S1
S5
IPADDRESS_A
KEY_AB
VPN CLIENT UNIT D
102
PUBLICKEY_D or HASH_D
IPADDRESS_D
PRIVATEKEY_D
IPADDRESS_B
IPADDRESS_C
KEY_DB
S9
S7
S3(S8)
IPADDRESS_B
DNS
105
MEDIATING APPARATUS S
104
S4
IPADDRESS_B
IPADDRESS_C
KEY_AB
PUBLICKEY_A,
PUBLICKEY_B
S2
S6
CERT
PUBLICKEY_A or HASH_A
IPADDRESS_A
PRIVATEKEY_A
VPN CLIENT UNIT A
101
100 WAN

FIG. 2

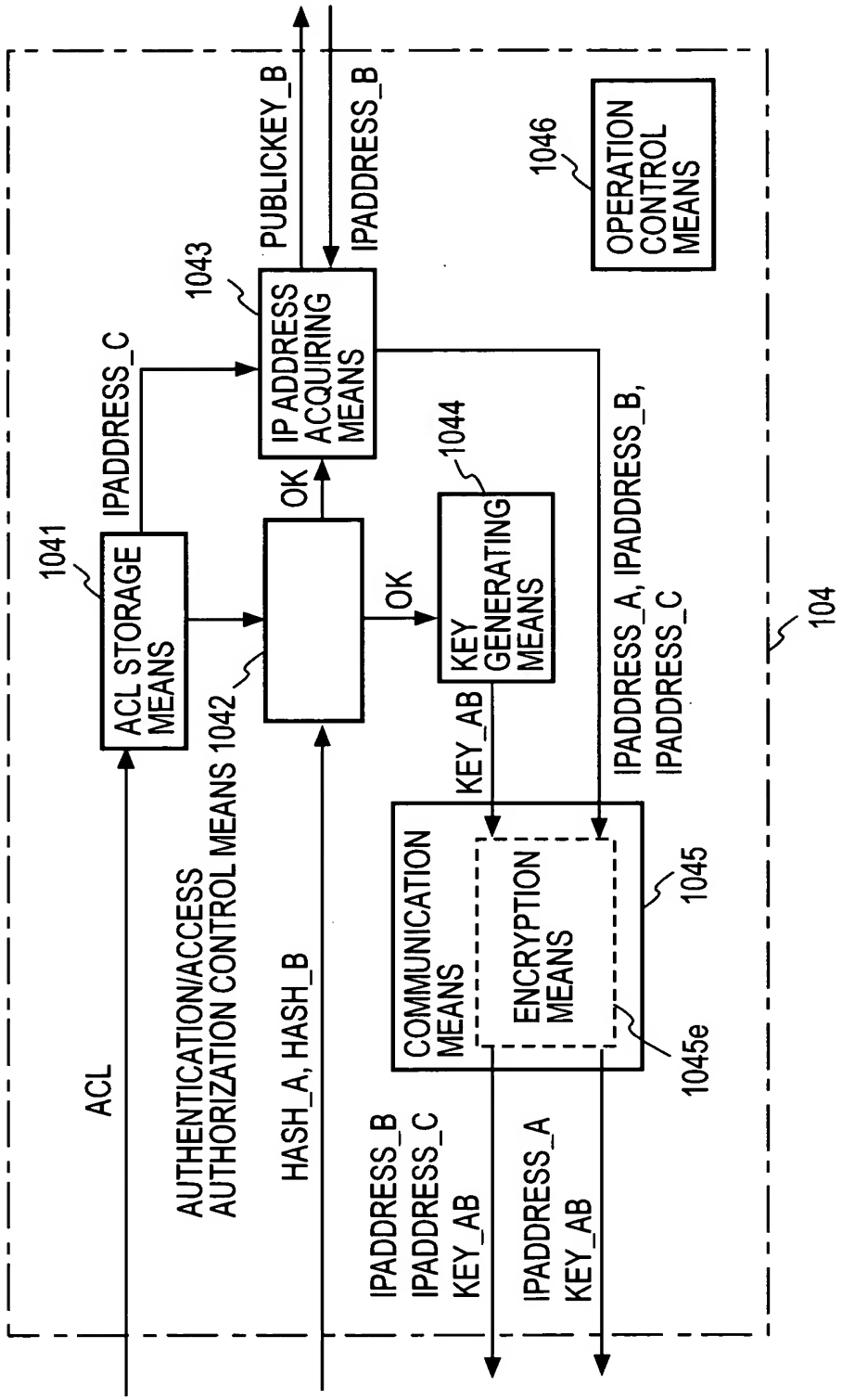

ACL
AUTHENTICATION/ACCESS AUTHORIZATION CONTROL MEANS 1042
HASH_A, HASH_B
IPADDRESS_B
IPADDRESS_C
KEY_AB
IPADDRESS_A
KEY_AB
COMMUNICATION MEANS
ENCRYPTION MEANS
1045
1045e
KEY_AB
IPADDRESS_A, IPADDRESS_B, IPADDRESS_C
OK
OK
1041
ACL STORAGE MEANS
IPADDRESS_C
1043
IP ADDRESS ACQUIRING MEANS
PUBLICKEY_B
IPADDRESS_B
1044
KEY GENERATING MEANS
1046
OPERATION CONTROL MEANS
104

FIG. 3

FIG. 4A

1041T

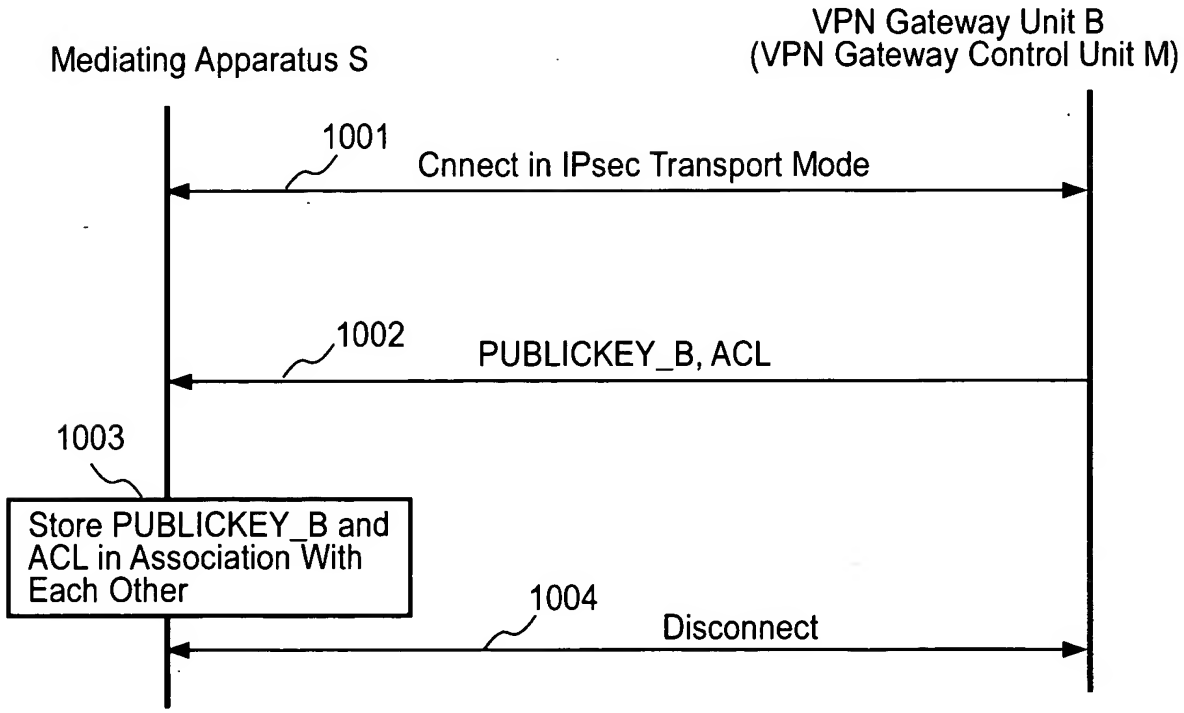
HASH_B	ACL
HASH_B1	ACL1
HASH_B2	ACL2
⋮	⋮

FIG. 4B

ACL1

ACCESS OBJECT	ACCESS SUBJECT
IPADDRESS_C1	HASH_A
IPADDRESS_C2	HASH_D
⋮	⋮

FIG. 5



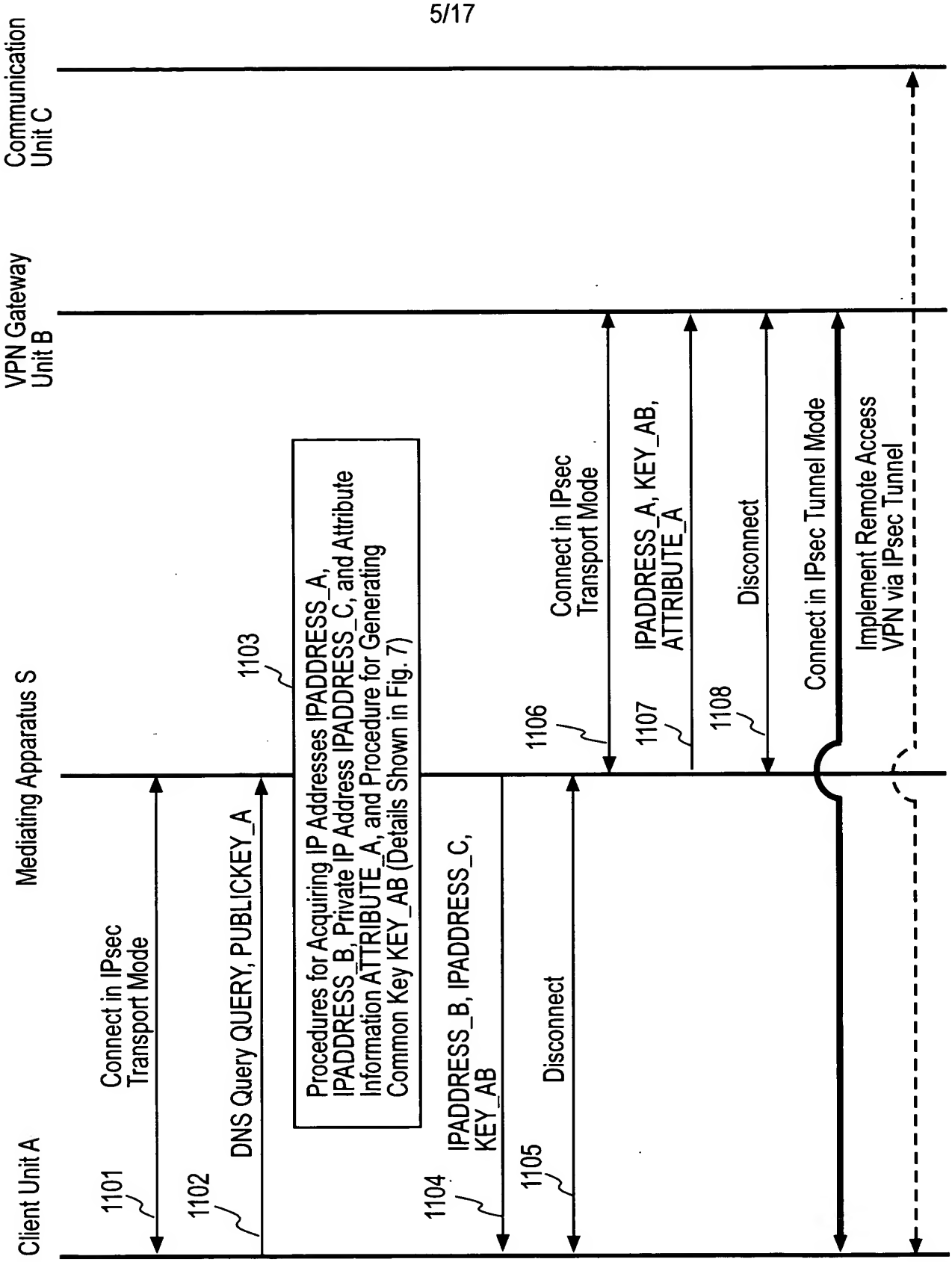

VPN Client Unit A
Mediating Apparatus S
VPN Gateway Unit B
Communication Unit C
1101
Connect in IPsec Transport Mode
1102
DNS Query QUERY, PUBLICKEY_A
1103
Procedures for Acquiring IP Addresses IPADDRESS_A, IPADDRESS_B, Private IP Address IPADDRESS_C, and Attribute Information ATTRIBUTE_A, and Procedure for Generating Common Key KEY_AB (Details Shown in Fig. 7)
1104
IPADDRESS_B, IPADDRESS_C, KEY_AB
1105
Disconnect
1106
Connect in IPsec Transport Mode
1107
IPADDRESS_A, KEY_AB, ATTRIBUTE_A
1108
Disconnect
Connect in IPsec Tunnel Mode
Implement Remote Access VPN via IPsec Tunnel

FIG. 6

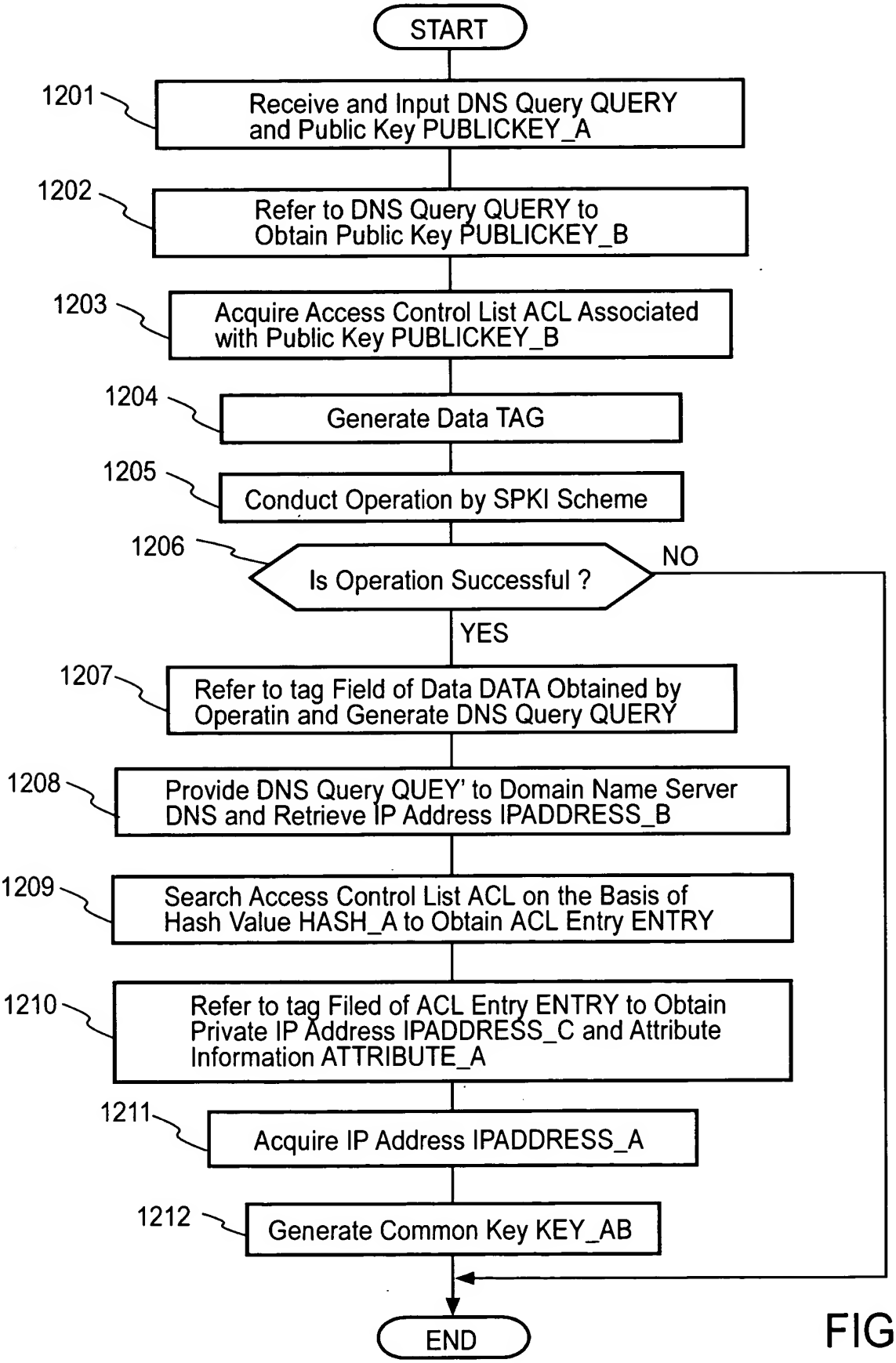

START
1201
Receive and Input DNS Query QUERY and Public Key PUBLICKEY_A
1202
Refer to DNS Query QUERY to Obtain Public Key PUBLICKEY_B
1203
Acquire Access Control List ACL Associated with Public Key PUBLICKEY_B
1204
Generate Data TAG
1205
Conduct Operation by SPKI Scheme
1206
Is Operation Successful ?
NO
YES
1207
Refer to tag Field of Data DATA Obtained by Operatin and Generate DNS Query QUERY
1208
Provide DNS Query QUEY' to Domain Name Server DNS and Retrieve IP Address IPADDRESS_B
1209
Search Access Control List ACL on the Basis of Hash Value HASH_A to Obtain ACL Entry ENTRY
1210
Refer to tag Filed of ACL Entry ENTRY to Obtain Private IP Address IPADDRESS_C and Attribute Information ATTRIBUTE_A
1211
Acquire IP Address IPADDRESS_A
1212
Generate Common Key KEY_AB
END

FIG. 7

FIG. 8

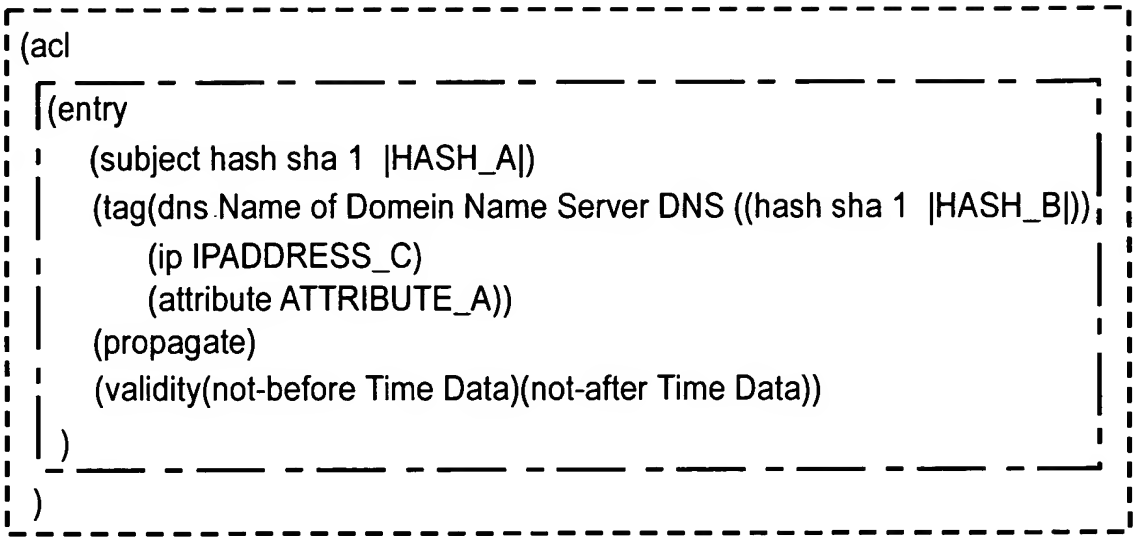
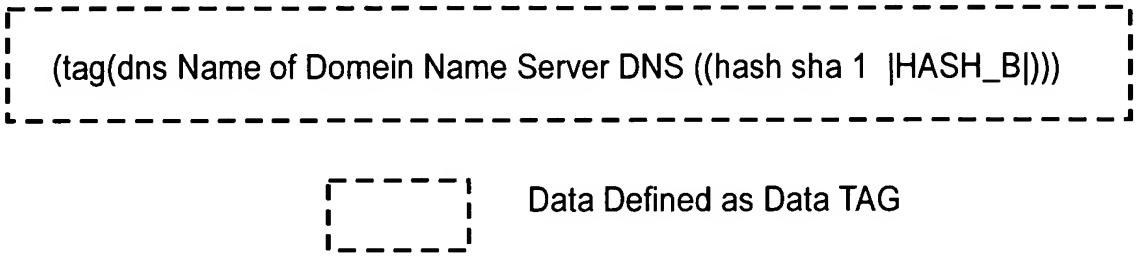

(acl
(entry
(subject hash sha 1 |HASH_A|)
(tag(dns Name of Domein Name Server DNS ((hash sha 1 |HASH_B|))
(ip IPADDRESS_C)
(attribute ATTRIBUTE_A))
(propagate)
(validity(not-before Time Data)(not-after Time Data))
)
)

FIG. 9


(tag(dns Name of Domein Name Server DNS ((hash sha 1 |HASH_B|)))
Data Defined as Data TAG

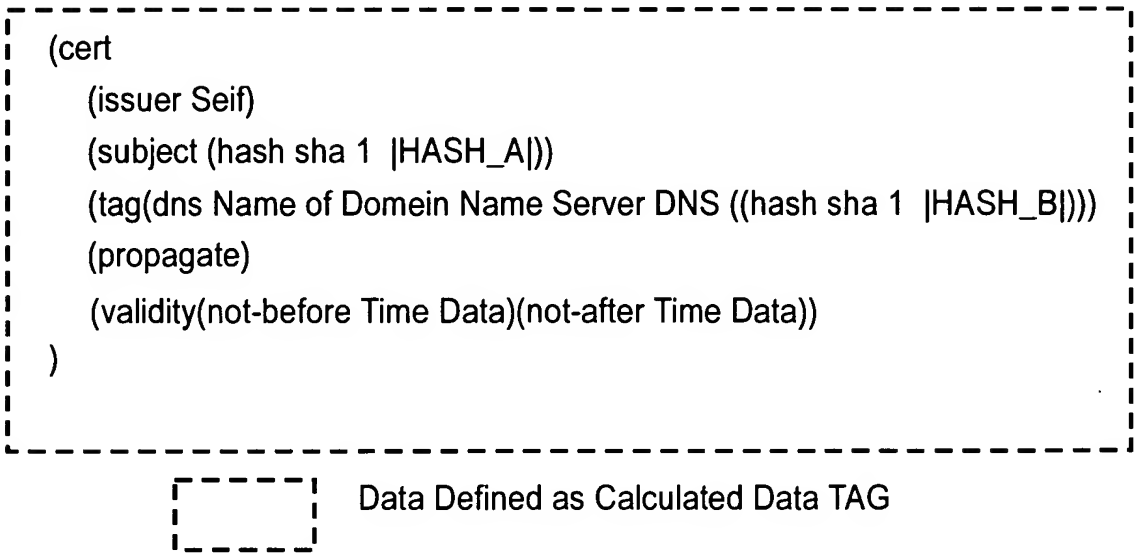

(cert
(issuer Seif)
(subject (hash sha 1 |HASH_A|))
(tag(dns Name of Domein Name Server DNS ((hash sha 1 |HASH_B|)))
(propagate)
(validity(not-before Time Data)(not-after Time Data))
)
Data Defined as Calculated Data TAG

FIG. 10

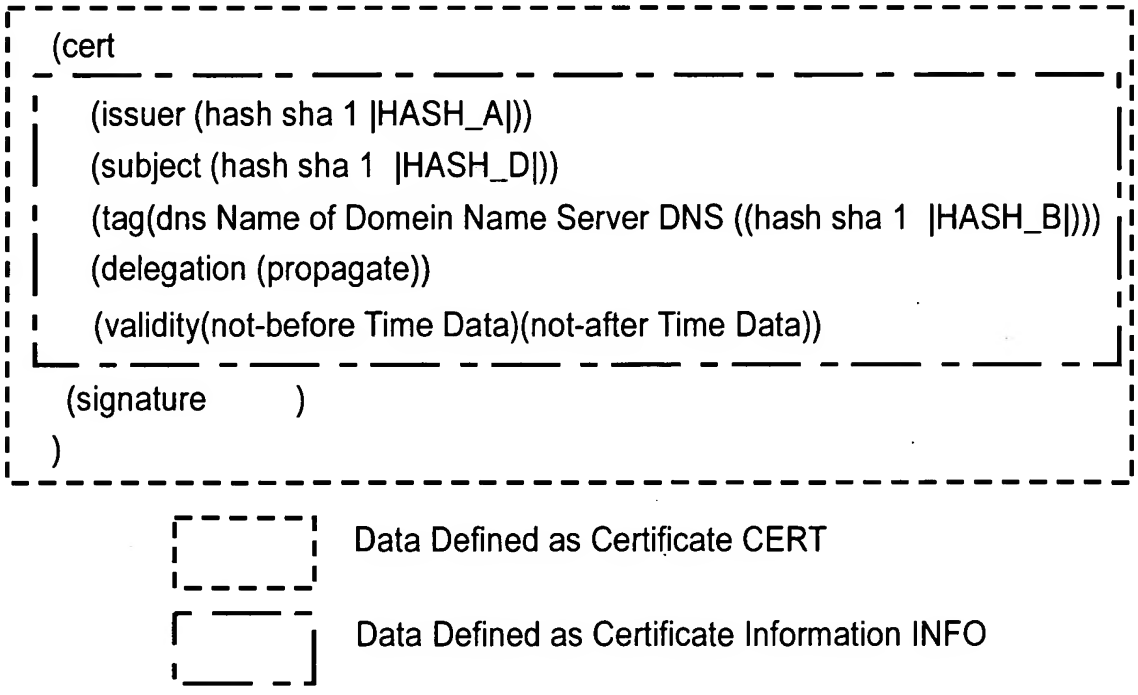

(cert
(issuer (hash sha 1 |HASH_A|))
(subject (hash sha 1 |HASH_D|))
(tag(dns Name of Domein Name Server DNS ((hash sha 1 |HASH_B|)))
(delegation (propagate))
(validity(not-before Time Data)(not-after Time Data))
(signature)
)
Data Defined as Certificate CERT
Data Defined as Certificate Information INFO

FIG. 11

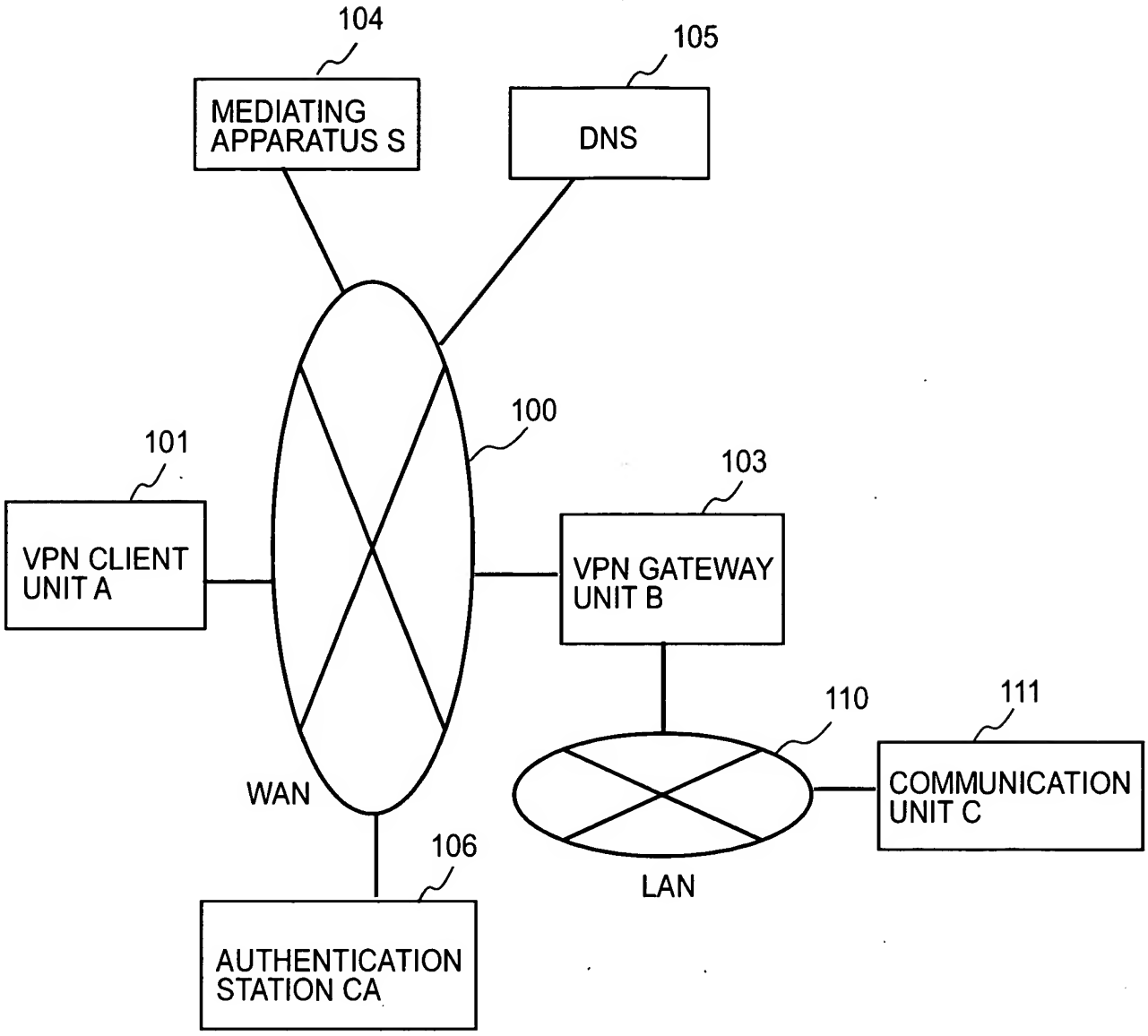

104
MEDIATING APPARATUS S
105
DNS
100
101
VPN CLIENT UNIT A
103
VPN GATEWAY UNIT B
110
111
COMMUNICATION UNIT C
WAN
LAN
106
AUTHENTICATION STATION CA

FIG. 12

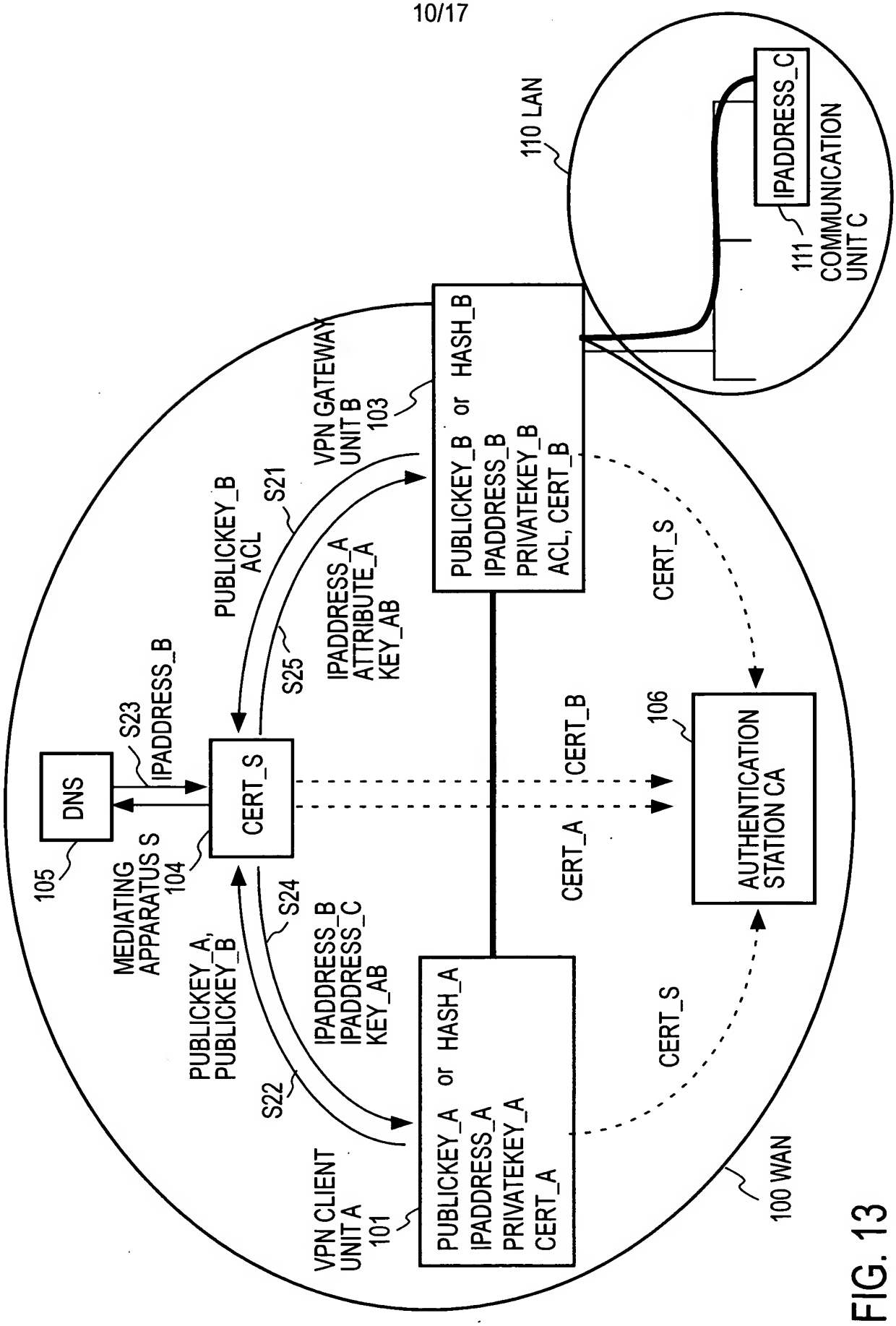

100 WAN
110 LAN
IPADDRESS_C
111 COMMUNICATION UNIT C
VPN GATEWAY UNIT B 103
PUBLICKEY_B or HASH_B
IPADDRESS_B
PRIVATEKEY_B
ACL, CERT_B
S21
PUBLICKEY_B ACL
S25
IPADDRESS_A ATTRIBUTE_A KEY_AB
CERT_S
DNS
105
S23
IPADDRESS_B
MEDIATING APPARATUS S 104
CERT_S
CERT_B
106
AUTHENTICATION STATION CA
CERT_A
S24
IPADDRESS_B IPADDRESS_C KEY_AB
PUBLICKEY_A, PUBLICKEY_B
S22
CERT_S
VPN CLIENT UNIT A 101
PUBLICKEY_A or HASH_A
IPADDRESS_A
PRIVATEKEY_A
CERT_A

FIG. 13

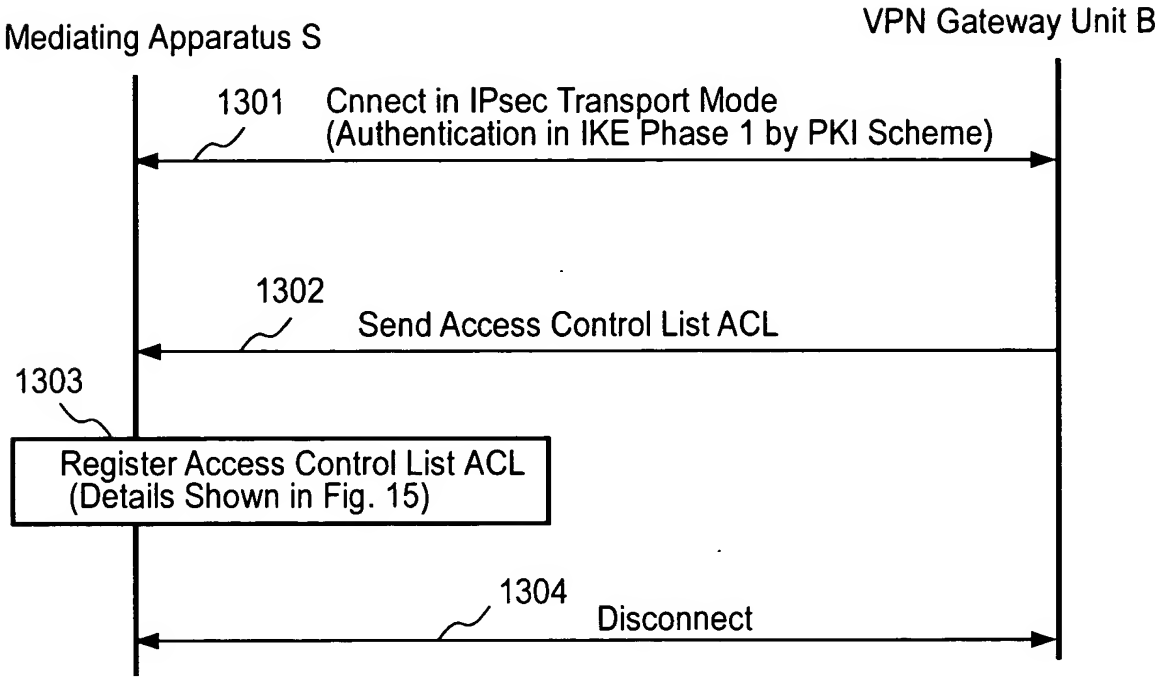

Mediating Apparatus S
VPN Gateway Unit B
1301
Cnnect in IPsec Transport Mode
(Authentication in IKE Phase 1 by PKI Scheme)
1302
Send Access Control List ACL
1303
Register Access Control List ACL
(Details Shown in Fig. 15)
1304
Disconnect

FIG. 14

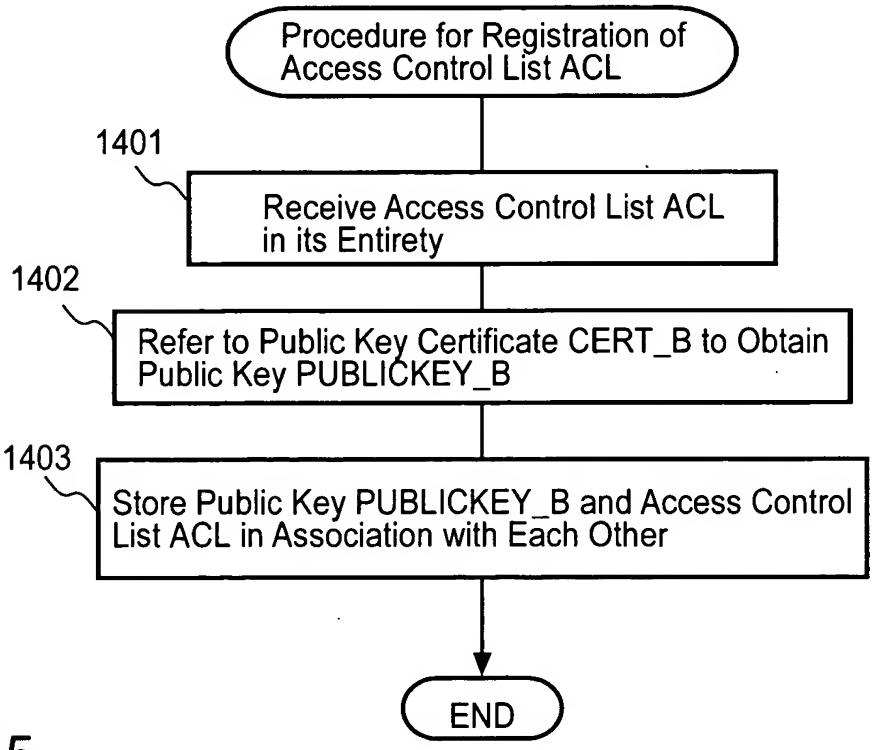

Procedure for Registration of
Access Control List ACL
1401
Receive Access Control List ACL
in its Entirety
1402
Refer to Public Key Certificate CERT_B to Obtain
Public Key PUBLICKEY_B
1403
Store Public Key PUBLICKEY_B and Access Control
List ACL in Association with Each Other
END

FIG. 15

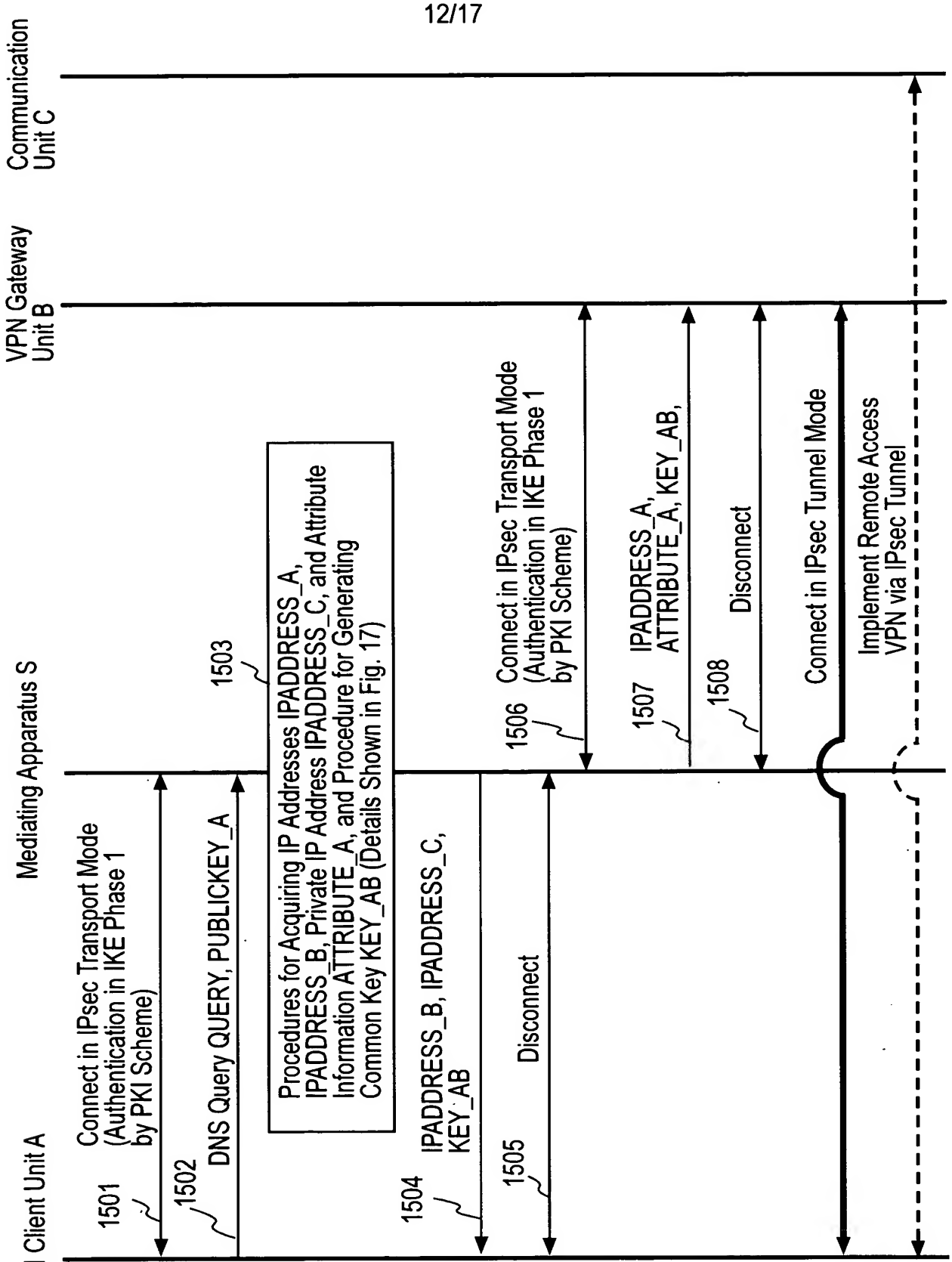

VPN Client Unit A
Mediating Apparatus S
VPN Gateway Unit B
Communication Unit C
1501
Connect in IPsec Transport Mode (Authentication in IKE Phase 1 by PKI Scheme)
1502
DNS Query QUERY, PUBLICKEY_A
1503
Procedures for Acquiring IP Addresses IPADDRESS_A, IPADDRESS_B, Private IP Address IPADDRESS_C, and Attribute Information ATTRIBUTE_A, and Procedure for Generating Common Key KEY_AB (Details Shown in Fig. 17)
1504
IPADDRESS_B, IPADDRESS_C, KEY_AB
1505
Disconnect
1506
Connect in IPsec Transport Mode (Authentication in IKE Phase 1 by PKI Scheme)
1507
IPADDRESS_A, ATTRIBUTE_A, KEY_AB,
1508
Disconnect
Connect in IPsec Tunnel Mode
Implement Remote Access VPN via IPsec Tunnel

FIG. 16

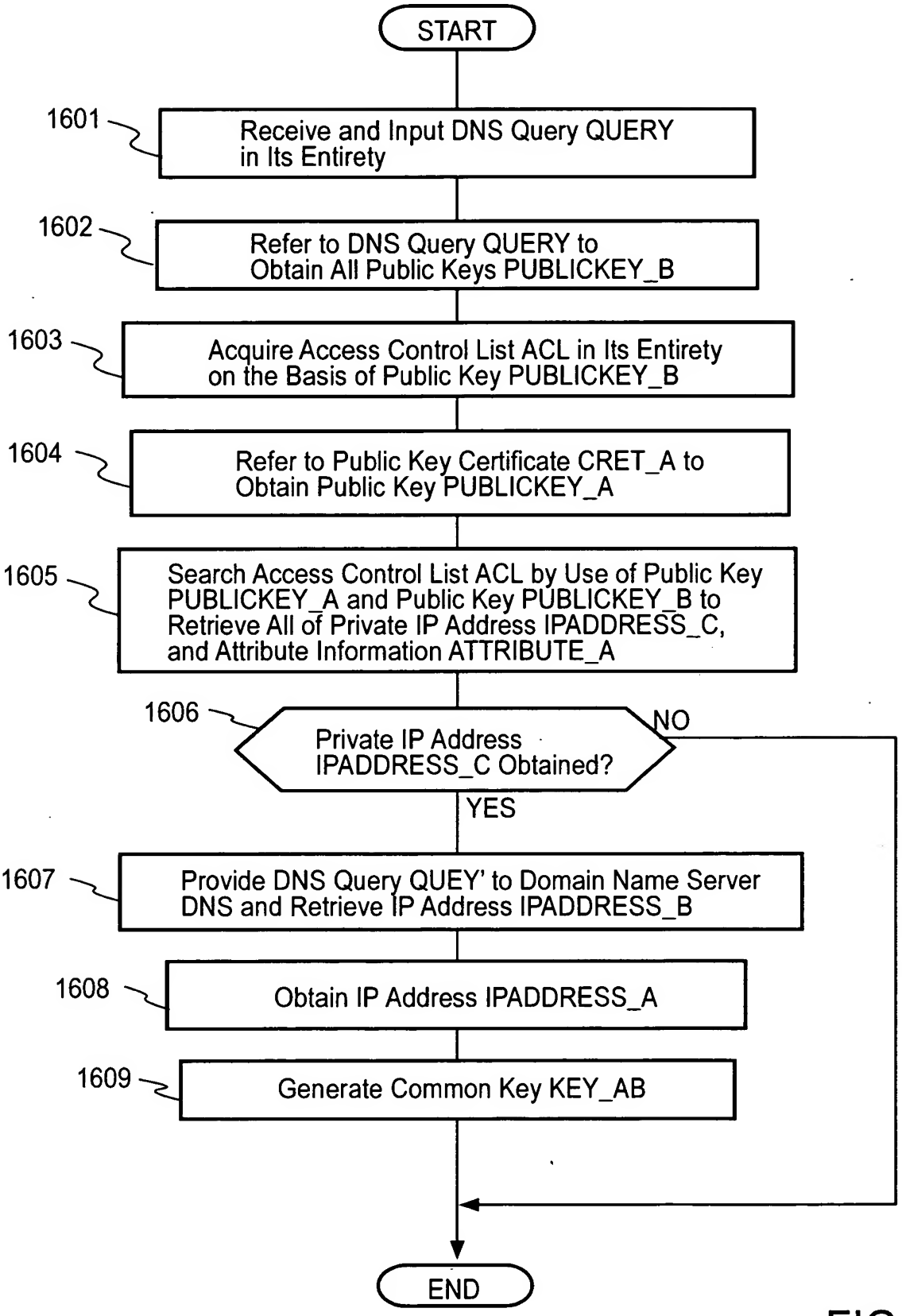

START
1601
Receive and Input DNS Query QUERY in Its Entirety
1602
Refer to DNS Query QUERY to Obtain All Public Keys PUBLICKEY_B
1603
Acquire Access Control List ACL in Its Entirety on the Basis of Public Key PUBLICKEY_B
1604
Refer to Public Key Certificate CRET_A to Obtain Public Key PUBLICKEY_A
1605
Search Access Control List ACL by Use of Public Key PUBLICKEY_A and Public Key PUBLICKEY_B to Retrieve All of Private IP Address IPADDRESS_C, and Attribute Information ATTRIBUTE_A
1606
Private IP Address IPADDRESS_C Obtained?
NO
YES
1607
Provide DNS Query QUEY' to Domain Name Server DNS and Retrieve IP Address IPADDRESS_B
1608
Obtain IP Address IPADDRESS_A
1609
Generate Common Key KEY_AB
END

FIG. 17

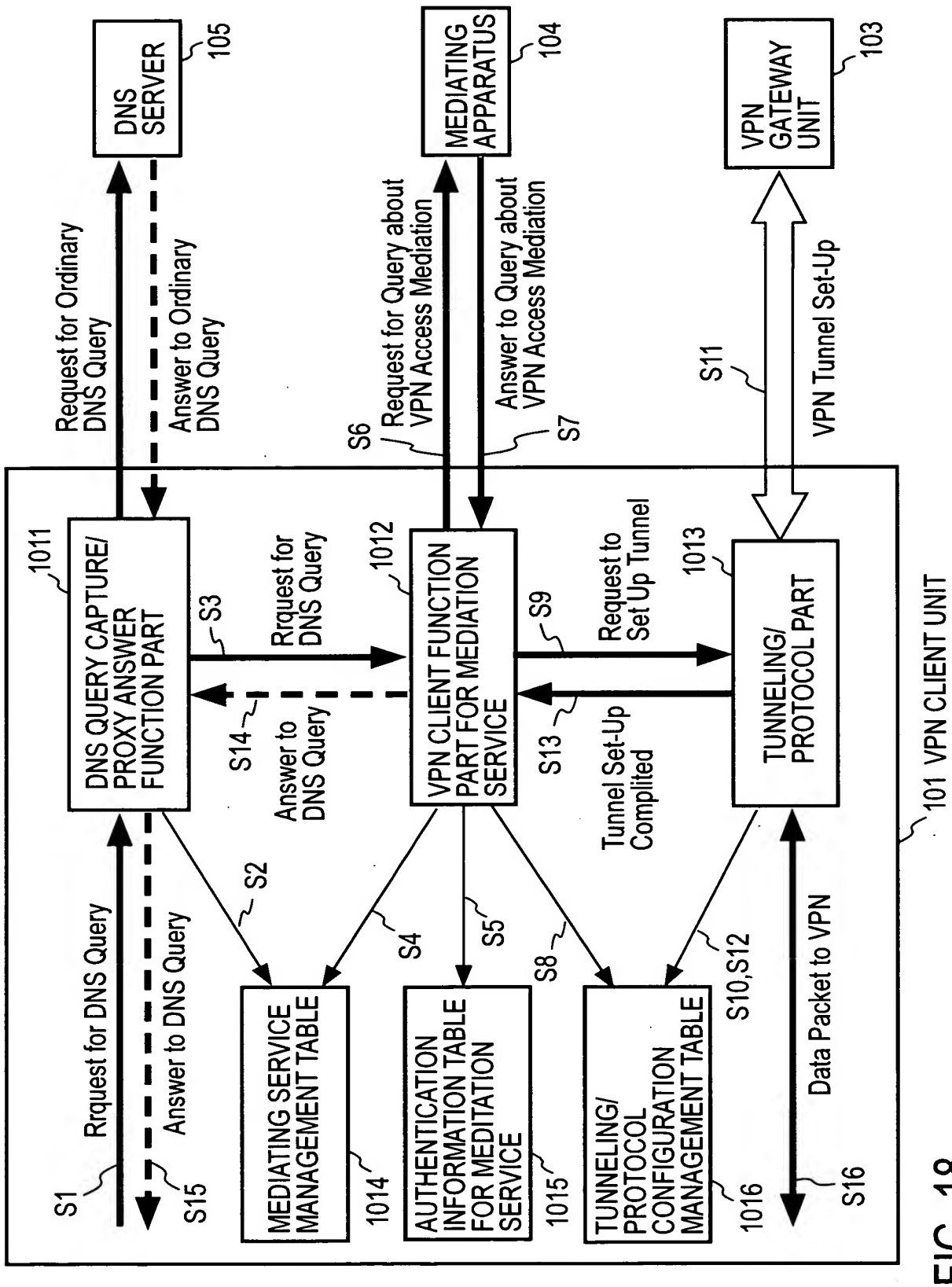

DNS SERVER
105
MEDIATING APPARATUS
104
VPN GATEWAY UNIT
103
Request for Ordinary DNS Query
Answer to Ordinary DNS Query
S6
Request for Query about VPN Access Mediation
Answer to Query about VPN Access Mediation
S7
S11
VPN Tunnel Set-Up
1011
DNS QUERY CAPTURE/ PROXY ANSWER FUNCTION PART
S3
Rrquest for DNS Query
1012
VPN CLIENT FUNCTION PART FOR MEDIATION SERVICE
S9
Request to Set Up Tunnel
1013
TUNNELING/ PROTOCOL PART
S14
Answer to DNS Query
S13
Tunnel Set-Up Complited
101 VPN CLIENT UNIT
S1
Rrquest for DNS Query
S15
Answer to DNS Query
S2
S4
S5
S8
S10,S12
Data Packet to VPN
S16
MEDIATING SERVICE MANAGEMENT TABLE
1014
AUTHENTICATION INFORMATION TABLE FOR MEDITATION SERVICE
1015
TUNNELING/ PROTOCOL CONFIGURATION MANAGEMENT TABLE
1016

FIG. 18

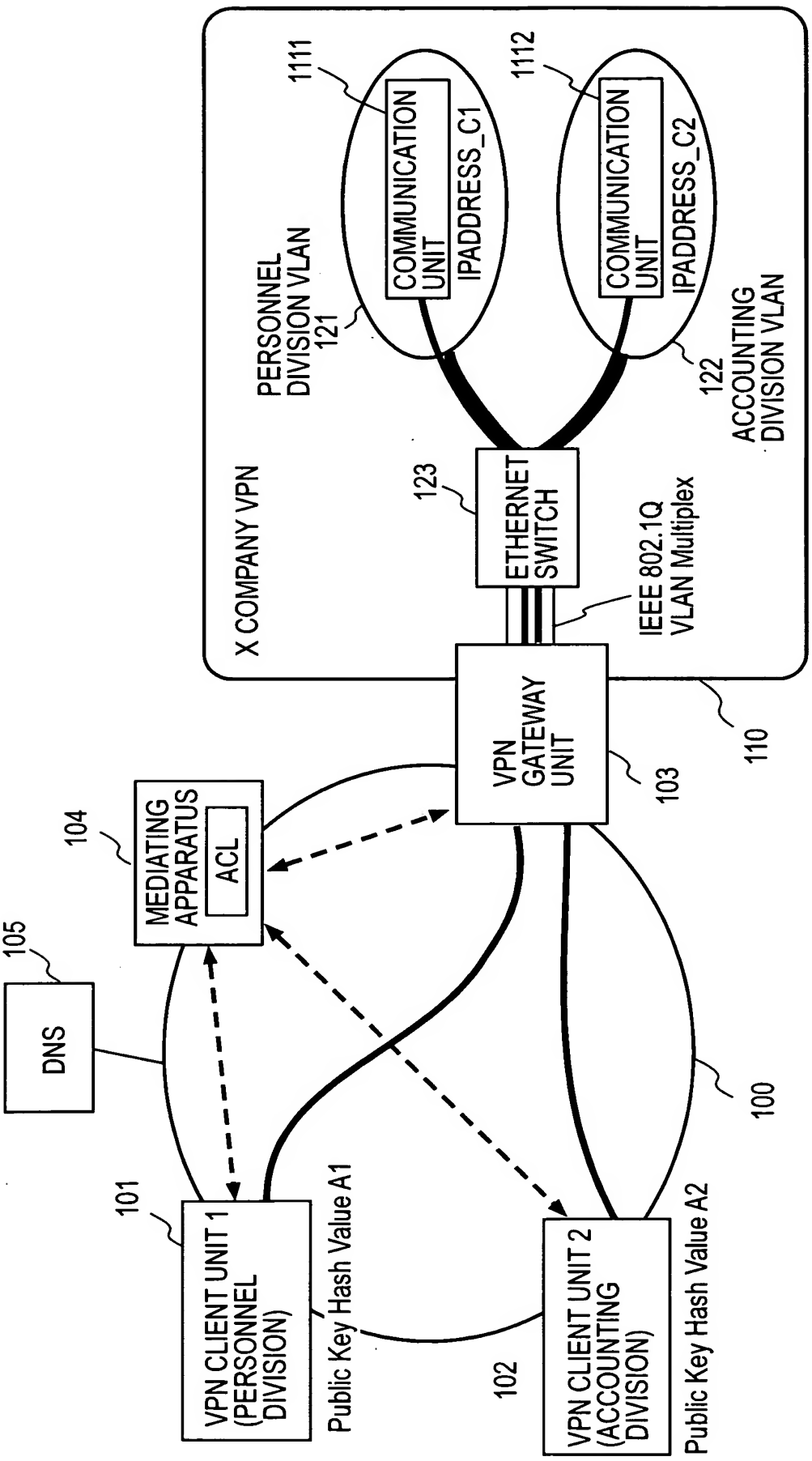

X COMPANY VPN
PERSONNEL DIVISION VLAN
121
1111
COMMUNICATION UNIT
IPADDRESS_C1
1112
COMMUNICATION UNIT
IPADDRESS_C2
122
ACCOUNTING DIVISION VLAN
123
ETHERNET SWITCH
IEEE 802.1Q VLAN Multiplex
VPN GATEWAY UNIT
103
110
MEDIATING APPARATUS
ACL
104
105
DNS
100
101
VPN CLIENT UNIT 1 (PERSONNEL DIVISION)
Public Key Hash Value A1
102
VPN CLIENT UNIT 2 (ACCOUNTING DIVISION)
Public Key Hash Value A2

FIG. 19

```
(acl                                                    Entry for VPN Client Unit A1
 (entry
    (subject hash sha1  |HASH_A1|)
    (tag(dns Name of Domain Name Server (hash sha1  |HASH_B|))
       (ip IPADDRESS_C1)
       (attribute(VLAN Personel Division VLAN)))
    (propagate)
    (validity(not-before time data)(not-after time data))
 )
                                                        Entry for VPN Client Unit A2
 (entry
    (subject hash sha1  |HASH_A2|)
    (tag(dns Name of Domain Name Server (hash sha1  |HASH_B|))
       (ip IPADDRESS_C2)
       (attribute(VLAN Accounting Division VLAN)))
    (propagate)
    (validity(not-before time data)(not-after time data))
 )
)
```

FIG. 20

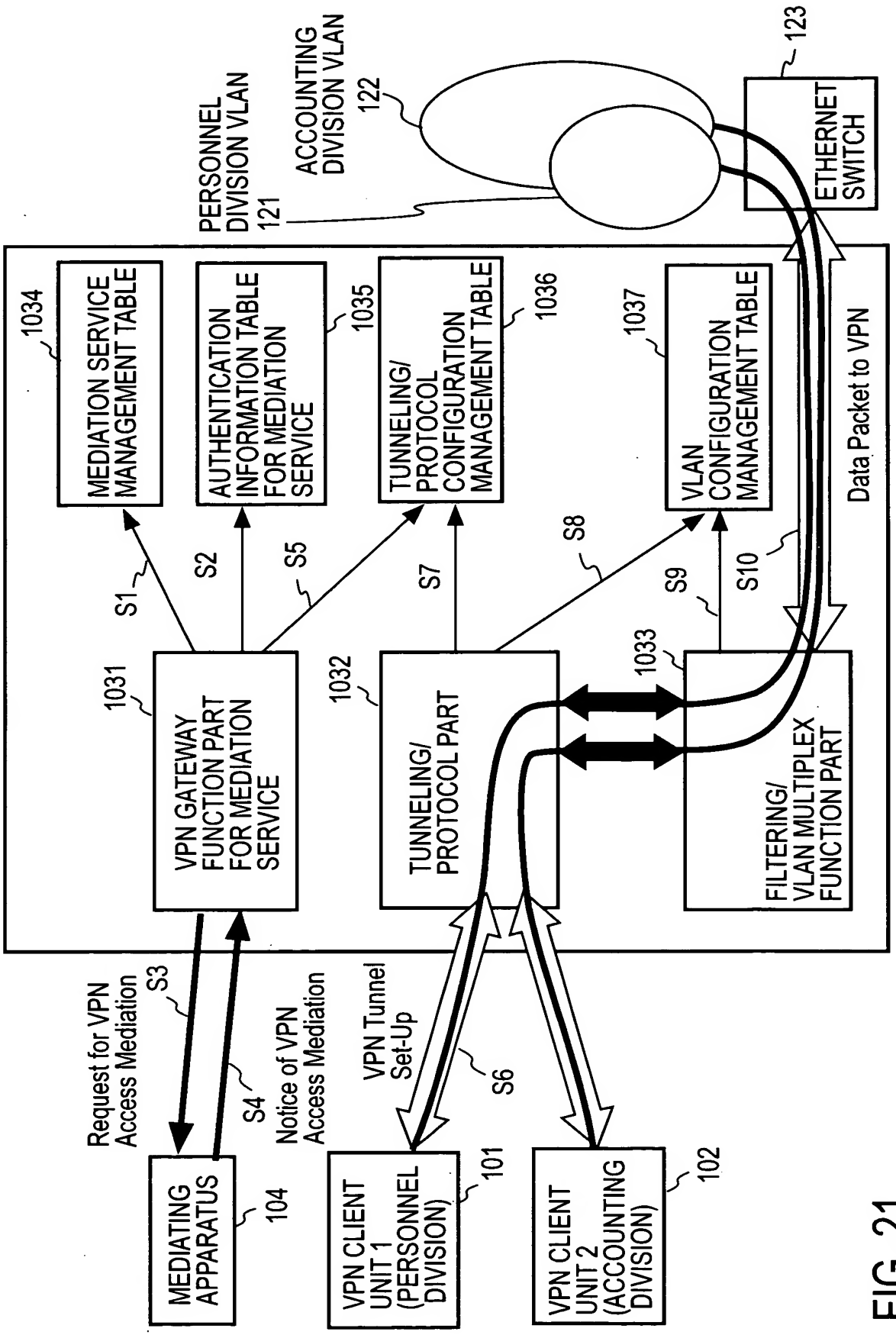

PERSONNEL DIVISION VLAN
121
ACCOUNTING DIVISION VLAN
122
123
ETHERNET SWITCH
1034
MEDIATION SERVICE MANAGEMENT TABLE
AUTHENTICATION INFORMATION TABLE FOR MEDIATION SERVICE
1035
TUNNELING/ PROTOCOL CONFIGURATION MANAGEMENT TABLE
1036
1037
VLAN CONFIGURATION MANAGEMENT TABLE
Data Packet to VPN
S1
S2
S5
S7
S8
S9
S10
1031
VPN GATEWAY FUNCTION PART FOR MEDIATION SERVICE
1032
TUNNELING/ PROTOCOL PART
1033
FILTERING/ VLAN MULTIPLEX FUNCTION PART
Request for VPN Access Mediation
S3
S4
Notice of VPN Access Mediation
VPN Tunnel Set-Up
S6
MEDIATING APPARATUS
104
VPN CLIENT UNIT 1 (PERSONNEL DIVISION)
101
VPN CLIENT UNIT 2 (ACCOUNTING DIVISION)
102

FIG. 21